REMARKS

Reconsideration and allowance of this application are respectfully requested. Claim 7 is cancelled. Claims 1-6 and 8-13 remain in this application and, as amended herein, are submitted for the Examiner's reconsideration.

Claim 6 has been amended to correct a minor grammatical error. No new issues that require further consideration or search are presented. It is therefore submitted that this Amendment should be entered.

In the Office Action, the Examiner rejected claims 1-6 and 8-13 under 35 U.S.C. § 103(a) as being unpatentable over Yoshiura (U.S. Patent No. 6,131,162) in view of Iida (U.S. Patent No. 6,209,787). Applicant submits that the claims are patentably distinguishable over the cited references.

The Yoshiura patent describes the distribution of content from a provider system to a purchaser system as follows: Before content is distributed, the purchaser system generates a signature key (private key) and a verification key (public key) and stores the signature key. Then, *the purchaser system sends the verification key to the provider system.* The provider system then *encrypts the stored content using the transmitted verification key* and sends the encrypted content to the purchaser system. The purchaser system next decrypts the encrypted content using the stored signature key *that was previously generated and stored by the purchaser system.* The purchaser system then generates a digital signature of the decrypted content using the signature key, and embeds the digital signature into the decrypted content. If the content is illegally copied, subsequently seized, and then stored in the provider system, the provider system extracts the digital signature from the content, and a *signature verifying module* of the provider system matches the digital signature *to identify the purchaser who made the illegal copy.* (See Figs. 2, 5 and 6;

col. 13, lines 1-17, 20-36, 43-45, and 50-55; Col. 13, line 61 - col. 14, line 3; and col. 14, lines 12-35).

Yoshiura therefore describes a signature verifying module that receives a digital signature *extracted from seized content*. (See Col. 13, line 61 - col. 14, line 3). Yoshiura does not disclose or suggest that the signature verifying module receives authentication information *from the purchaser system*, and Yoshiura does not disclose or suggest that the signature verifying module receives authentication information *when the purchaser system requests permission to receive the encrypted content*.

Yoshiura then describes that the signature verifying module matches the digital signature to a stored value *to identify the purchaser who made the illegal copy*. (See col. 14, lines 12-35). Yoshiura not disclose or suggest that the signature verifying module determines whether the authentication information *is valid*.

The Iida patent describes a system that allows for the selection of musical compositions, the editing of the selection of musical compositions and related information, the storing of the edited musical compositions and related information in a recording medium, and the purchase of the recording medium. (See Abstract, and col. 1, lines 10-16). The Iida patent does not remedy the above-described deficiencies of Yoshiura.

Therefore, neither Yoshiura nor Iida suggests:

> an authentication unit operable to receive authentication information from the another apparatus when the another apparatus requests permission to receive the encrypted content and to determine whether the authentication information is valid;

as recited in claim 1.

Yoshiura also describes that the controlling module *of the purchaser system* sends a verification key *to the provider system*. The provider system *does not send* a key to the

purchaser system. (See col. 13, lines 12-14). Therefore, Yoshiura not disclose or suggest a transmitting unit (of the system that carries out secure transmission of content) operable to transmit a decryption key to the another apparatus (i.e., the apparatus that is to receive the content).

Moreover, Yoshiura describes that the purchaser system sends the verification key to the provider system *before any identification is carried out by the* purchaser system. (See col. 13, lines 1-13). Yoshiura not disclose or suggest transmitting a decryption key *when the authentication information is valid.*

Additionally, Yoshiura describes that the transmitted verification key is used by the provider system *to encrypt* the stored content. (See col. 13, lines 11-15). The patent also describes that the purchaser system decrypts the encrypted content using the stored signature key *that was previously generated and stored by the purchaser system.* (See col. 13, lines 17-36). Yoshiura not disclose or suggest *transmitting* a key is needed *to decrypt encrypted content.*

The Iida patent does not remedy any of these described deficiencies.

Therefore, neither Yoshiura nor Iida suggests:

> a transmitting unit operable to transmit a decryption key to the another apparatus when the authentication information is valid, the decryption key being needed to decrypt the encrypted content

as called for in claim 1.

It follows that neither Yoshiura nor Iida, whether taken alone or in combination, discloses or suggests the information processing apparatus defined in claim 1, and claim 1 is therefore patentably distinct and unobvious over the references.

Claims 2-3 and 12 depend from claim 1, and each claim further defines and limits the invention set out in the

independent claim. It follows that each of claims 2-3 and 12 defines a combination that is patentably distinguishable over the Yoshiura and Iida references at least for the same reasons.

Independent claim 4 defines a method for carrying out secure transmission of content from an information processing apparatus to another apparatus over a network. The claim calls for:

> receiving authentication information from the another apparatus when the another apparatus requests permission to receive the encrypted content;

and further calls for:

> transmitting a decryption key to the another apparatus when the authentication information is valid, the decryption key being needed to decrypt the encrypted content[.]

Therefore, for at least the same reasons, claim 4 is also patentably distinguishable over Yoshiura and Iida.

Independent claim 5 relates to a recording medium having recorded thereon a program for executing the method recited in claim 4. For at least the same reasons, Claim 5 is also patentably distinguishable over the references.

Independent claim 6 defines an information processing apparatus that includes:

> a first transmitting unit operable to transmit to the first apparatus a request for permission to receive the content[.]

Yoshiura does not disclose or suggest that the purchaser system transmits a request for permission to receive the content, and Iida does not address this deficiency.

Claim 6 also recites:

> a second authentication unit operable to receive authentication information from the second apparatus when a request for permission to receive the content is made from the second apparatus and to determine whether the authentication information is valid;

and further recites:

> a second transmitting unit operable to transmit a second decryption key to the second apparatus when the authentication information is valid, the second decryption key being needed to decrypt the reencrypted content[.]

Claim 6 is therefore also patentably distinguishable over Yoshiura and Iida for at least the reasons set out above regarding claim 1.

Claims 8-9 and 13 depend from claim 6 and are also distinguishable over the references for at least the same reasons.

Independent claim 10 is directed to a method for carrying out secure receiving of content from a first apparatus over a first network and for carrying out secure transmission of content to a second apparatus over a second network. Claim 10 includes steps having limitations similar to those set out in claim 4. Therefore, claim 10 is patentably distinguishable over Yoshiura and Iida at least for the same reasons.

Independent claim 11 relates to a recording medium having recorded thereon a program for executing the method defined in claim 10. Claim 11 is therefore distinguishable over the cited art for at least the same reasons.

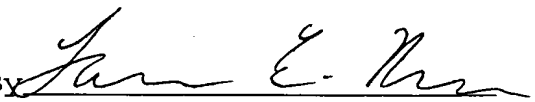
Accordingly, the withdrawal of the rejection under U.S.C. § 103(a) is respectfully requested.

In view of the above, each of the presently pending claims in this application is believed to be in immediate condition for allowance. Accordingly, the Examiner is respectfully requested to withdraw the outstanding rejection of the claims and to pass this application to issue. If, however, for any reason the Examiner does not believe that such action can be taken at this time, it is respectfully requested that the Examiner telephone applicant's attorney at (908) 654-5000 in order to overcome any additional objections which the Examiner might have.

If there are any additional charges in connection with this requested amendment, the Examiner is authorized to charge Deposit Account No. 12-1095 therefor.

Dated: November 23, 2005

Respectfully submitted,

By 

Lawrence E. Russ
Registration No.: 35,342
LERNER, DAVID, LITTENBERG,
KRUMHOLZ & MENTLIK, LLP
600 South Avenue West
Westfield, New Jersey 07090
(908) 654-5000
Attorney for Applicant

587534_1.DOC